



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/785,407	02/25/2004	Govindarajan Krishnamurthi	60282.00168	8359
32294	7590	08/09/2007	EXAMINER	
SQUIRE, SANDERS & DEMPSEY L.L.P. 14TH FLOOR 8000 TOWERS CRESCENT TYSONS CORNER, VA 22182			FARAGALLA, MICHAEL A	
		ART UNIT		PAPER NUMBER
		2617		
		MAIL DATE	DELIVERY MODE	
		08/09/2007	PAPER	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	10/785,407	KRISHNAMURTHI ET AL.
	Examiner	Art Unit
	Michael Faragalla	2617

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 09 May 2007.  
 2a) This action is FINAL.                            2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-18 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-18 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date _____	6) <input type="checkbox"/> Other: _____

## DETAILED ACTION

1. Applicant's arguments have been fully considered, and therefore, this action is made non final in view of the new grounds of rejection.

### *Claim Rejections - 35 USC § 112*

2. In response to applicant's arguments, the rejections under 112 second paragraph has been withdrawn.

### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

4. Claims 2,8,13, 17 and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by **Norefors et al (Patent number: US 6,370,380)**.

Consider **Claim 2**, Norefors et al show a method of validating information of a mobile node within a candidate access router discovery procedure in a mobile IP environment, said method comprising:

- (a) Generating a token by a first access router to which the mobile node was previously attached (figure 2; column 4, lines 30-40); (the old access point sends a token to the mobile device containing information about the old access point).
- (b) Sending the token from the first access router to the mobile node within a message comprising a list of candidate access routers (figure 2; column 4, lines 30-40); (the old access point sends a token to the mobile device containing information about the old access point as well as information about the new access point).
- (c) Sending a token from the mobile node to a second access router as selected candidate after handover procedure between the first and second access routers (figure 1; column 4, lines 45-67); (the mobile device sends a message to the new access point in order to decipher items within).
- (d) Sending the token within an exchange between the access routers specific to the discovery procedure from the second access router back to the first access router for verification (column 3, lines 60-67; column 4, lines 1-23).

Consider **Claim 8**, Norefors et al show a system for validating information of a mobile node within a candidate access router discovery procedure in a mobile IP environment, the system comprising:

- (a) A first router, said mobile node and a second access router (see figure 1).

(b) Wherein, the first access router includes a generating unit configured to generate a token, first sending unit configured to send the token to the mobile node within a message comprising a list of candidate access routers (figure 2; column 4, lines 30-40); (the old access point sends a token to the mobile device containing information about the old access point).

(c) Wherein the mobile node includes second sending unit configured to send the token to the second access router as selected candidate after a handover procedure between the access routers (figure 1; column 4, lines 45-67); (the mobile device sends a message to the new access point in order to decipher items within).

(d) The second access router includes third sending unit configured to send the token within an exchange between the access routers specific to the discovery procedure back to the first access router and a verification unit configured to verify the token (column 3, lines 60-67; column 4, lines 1-23).

Consider **Claim 13**, Norefors et al show an access router for validating information of a mobile node in a mobile IP, comprising:

(a) A generating unit to generate a token; a first sending unit configured to send the token to the mobile node within a message comprising a list of candidate access routers (figure 2; column 4, lines 30-40); (the old access point sends a token to the mobile device containing information about the old access point as well as information about the new access point).

(b) A second sending unit configured to send the token within an exchange with another access router specific to the discovery procedure to the other access router and a verification unit configured to verify a token (column 3, lines 60-67; column 4, lines 1-23).

Consider **Claim 17**, Norefors et al show a system for validating information of a mobile node within a candidate access router discovery procedure in a mobile IP environment, comprising;

(a) A first router said mobile node and a second access router (see figure 1), wherein, the first access router includes generating means for generating a token, first sending means for sending the token to the mobile node within a message comprising a list of candidate access routers (figure 2; column 4, lines 30-40); (the old access point sends a token to the mobile device containing information about the old access point as well as information about the new access point).

(b) The mobile node includes second sending means for sending the token to the second access router as selected candidate after a handover procedure between the access routers (figure 1; column 4, lines 45-67); (the mobile device sends a message to the new access point in order to decipher items within).

(c) The second access router includes third sending means for sending the token within an exchange between the access routers specific to the discovery procedure back to the first access router and verification means for verifying the token (column 3, lines 60-67; column 4, lines 1-23).

Consider **Claim 18**, Norefors et al show an apparatus for validating information of a mobile node in a mobile IP, comprising:

- (a) Generating means for generating a token; first sending means for sending the token to the mobile node within a message comprising a list of candidate access routers (figure 2; column 4, lines 30-40); (the old access point sends a token to the mobile device containing information about the old access point as well as information about the new access point).
- (b) Second sending means for sending the token within an exchange with another access router specific to the discovery procedure to the other access router; and verification means for verifying the token (column 3, lines 60-67; column 4, lines 1-23).

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

- (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims **1,3-5,7,9,10,12,14-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Frid et al (Patent number: 6,137,791)** in view of **Norefors et al (Patent number: US 6,370,380)**.

Consider **Claim 1**, Frid et al shows a method of reducing denial-of-service attacks by malicious mobile nodes in a mobile IP environment, said method comprising:

- (a) Populating the cache with cache entries in response to actions initiated by mobile nodes (column 4, lines 36-48); (when a mobile travels into a geographical area, subscription data is stored regarding the mobile station).
- (b) Each cache entry is tagged with an identity of an action initiating mobile node, which identity is based on information that is verifiable by the access routers and which cannot be modified arbitrarily by the mobile node (read to be the IP address of the mobile terminal) (column 5, lines 10-15).
- (c) Wherein a total number of entries that can be tagged and thus introduced into a cache by any given node is limited (column 4, lines 36-48).

However, Frid et al does not specifically show that the method further comprising maintaining, by each of a plurality of access routers within the mobile IP environment, a cache of neighboring access routers as candidates and their associated access points. In related art, Norefors et al show the method further comprising maintaining, by each of a plurality of access routers within the mobile IP environment, a cache of neighboring access routers as candidates and their associated access points (figure 2; column 4,

lines 30-50); (the old access point sends a token message to the mobile device indicating the new access point).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors et al into the teaching of Frid et al in order to protect the system against intruders (Norefors et al ; column 1, lines 40-50).

Consider **Claim 7**, Frid et al shows a system for reducing denial-of-service attacks by malicious mobile nodes in a mobile IP environment, said system comprising:

(a) A plurality of mobile nodes which are capable of populating the caches in response to actions initiated (column 4, lines 36-48); (when a mobile travels into a geographical area, subscription data is stored regarding the mobile station).

(b) Wherein the cache is configured such that each cache entry is tagged with an identity of the action initiating mobile node having thus created the entry, and that a total number of entries that can be tagged and thus introduced into the cache by any given node is limited (column 4, lines 36-48).

However, Frid et al does not specifically show that a plurality of access routers within the mobile IP environment, each router maintaining a cache of neighboring access routers as candidates and their associated access points.

However, Frid et al does not specifically show that the method further comprising maintaining, by each of a plurality of access routers within the mobile IP environment, a cache of neighboring access routers as candidates and their associated access points.

In related art, Norefors et al show the method further comprising maintaining, by each of a plurality of access routers within the mobile IP environment, a cache of neighboring access routers as candidates and their associated access points (figure 2; column 4, lines 30-50); (the old access point sends a token message to the mobile device indicating the new access point).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors et al into the teaching of Frid et al in order to protect the system against intruders (Norefors et al ; column 1, lines 40-50).

Consider **Claim 12**, Frid et al shows an access router for reducing denial-of-service attacks by malicious mobile nodes in a mobile IP, said router comprising:

A cache is arranged such that each cache entry is tagged with the identity of the mobile node having initiated the entry creation, and the total number of entries that can be tagged and thus introduced into the cache by any given node is limited (column 4, lines 36-48).

However, Frid et al does not specifically show that the router comprising a cache of neighboring access routers as candidates and their associated access points.

In related art, Norefors et al show that the router comprising a cache of neighboring access routers as candidates and their associated access points (figure 2; column 4, lines 30-50); (the old access point sends a token message to the mobile device indicating the new access point).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors et al into the teaching of Frid et al in order to protect the system against intruders (Norefors et al ; column 1, lines 40-50).

Consider **Claim 3**, Frid et al in view of Norefors et al show the method of claim 1, wherein the identity of the mobile node is an international mobile subscriber identity (IMSI) for cellular communication systems, and a network access identifier (NAI) for systems based on Internet Protocol (IP).

Consider **Claims 4, 9, and 14** the combination of Frid et al and Norefors et al show the method according to claim 1, as well as the system of claim 7, as well as the access router according to claim 12, wherein an action initiated by a mobile node comprises a handover procedure of the mobile node between a previous access router, said method further comprising: generating a token by the previous first access router; sending the token from the previous access router to the mobile node within a message comprising a list of candidate access routers; sending the token within a message specific to the discovery procedure from the mobile node to the new access router as selected candidate after the handover procedure, sending the token within a neighbor exchange between the access routers resulting in cashe entries being created or refreshed from the second access router back to the first router access for verification.

Consider **Claims 5,10, and 15** Frid et al as modified by Norefors et al show the method according to claim 4, as well as the system of claim 9, as well as the access router of claim 14, but fail to specifically show that the token is generated by maintaining by the previous access router a short list of random values used as keys to hash the identity of the mobile node, each key in the short list is associated with an integer index that is passed along with the token, and wherein upon receiving the token for verification, the previous access router uses the integer index to lookup the associated key, hash the identity of the mobile node sent in the neighbor exchange and compares the hash to the token.

However, in related art, Norefors et al shows that the token is generated by maintaining by the previous access router a short list of random values used as keys to hash the identity of the mobile node, each key in the short list is associated with an integer index that is passed along with the token, and wherein upon receiving the token for verification, the previous access router uses the integer index to lookup the associated key, hash the identity of the mobile node sent in the neighbor exchange and compares the hash to the token (column 3, lines 46-67; figure 3).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors et al into the teaching of Frid et al in order to protect communications (Norefors et al, column 3, lines 63-65).

Consider **Claim 16**, Frid et al as modified by Norefors et al shows the access router according to claim 15, but fail to specifically show that the generating means are

configured to generate new keys with progressing time, to add them to the head of the list and remove old keys.

However, in related art, Norefors et al shows that the generating means are configured to generate new keys with progressing time, to add them to the head of the list and remove old keys (column 3, lines 60-67).

Therefore, it would have been obvious to a person skilled in the art at the time the invention was made to incorporate the teaching of Norefors et al into the teaching of Frid et al in order to protect communications (Norefors et al, column 3, lines 63-65).

### ***Conclusion***

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

(1) REUSE OF SECURITY ASSOCIATIONS FOR IMPROVING HAND OVER PERFORMANCE (**Patent number: US 6,418,130**).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Faragalla whose telephone number is (571) 270-1107. The examiner can normally be reached on Mon-Fri 7:30 am-5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nick Corsaro can be reached on (571) 272-7876. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Michael Faragalla



JOSEPH FEILD  
SUPERVISORY PATENT EXAMINER